Quadratic reciprocity in a finite group

William Duke and Kimberly Spears

1. Introduction

The law of quadratic reciprocity is a gem from number theory. In this article we show that it has a natural generalization to an arbitrary finite group. Our treatment relies on concepts and results known at least 100 years ago. See [**2**, Chapter I] for a beautiful exposition of the nineteenth century algebra and number theory we will take as known.

The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ of reduced residue classes modulo an odd prime p is a cyclic group of (even) order $p-1$. Thus it has a unique character of order 2. This character has a natural pull-back to $\mathbb{Z}$, which is a real Dirichlet character $(\mathrm{mod}\, p)$, called the Legendre symbol $\left(\frac{\cdot}{p}\right)$. By convention, $\left(\frac{a}{p}\right)=0$ if $p \mid a$ and otherwise we have that $\left(\frac{a}{p}\right)=1$ if and only if a is a square modulo p.

In 1872 Zolotarev [**9**] gave an interpretation of the Legendre symbol $\left(\frac{a}{p}\right)$ that is less well-known; it gives the sign of the permutation of the elements of $G=\mathbb{Z}/p\,\mathbb{Z}$ induced by multiplication by a, provided $p \nmid a$. To see this, first observe that this recipe defines a character on $(\mathbb{Z}/p\,\mathbb{Z})^*$. Furthermore, if it is not trivial, this character must have order 2 and hence be the Legendre symbol. But it is not trivial since a generator of $(\mathbb{Z}/p\,\mathbb{Z})^*$ induces a $(p-1)$-cycle, which is an odd permutation. Motivated by this observation, we will define in (4) below a quadratic symbol for any finite group G.

The classical law of quadratic reciprocity states that for $q \neq p$ another odd prime,

$$(1)\quad \left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),\quad \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}\quad\text{and}\quad \left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

This was first proven by Gauss in 1796 when he was nineteen years old. By 1818 he had published six proofs. The ideas behind his sixth proof [**5**] (see [**2**, p.19]), based on the Gauss sum, led to proofs of

The research of the second author was supported by UC LEADS.

quadratic reciprocity using the arithmetic of cyclotomic fields and the Frobenius automorphism, which was introduced in 1896 [**3**]. We will combine this classical technique with another invention of Frobenius from 1896 [**4**], the character table, to prove a law of reciprocity for the quadratic symbol for any finite group G. A corollary of our result, given in §3, implies classical quadratic reciprocity when $G = \mathbb{Z}/p\,\mathbb{Z}$ and also extends Zolotarev's observation to any group of odd order.

2. The Kronecker symbol

Before explaining this generalization, let us restate the law of quadratic reciprocity in one formula by introducing the Jacobi and Kronecker symbols. The Jacobi symbol simply extends the Legendre symbol to $\left(\frac{\cdot}{n}\right)$ for arbitrary odd $n \in \mathbb{Z}^+$ by multiplicativity, so that if $n = p_1 \cdots p_r$ is the factorization of n into (not necessarily distinct) primes,

$$\left(\tfrac{a}{n}\right) = \prod_{k=1}^{r} \left(\tfrac{a}{p_k}\right).$$

A discriminant is a non-zero[1] integer d with $d \equiv 0$ or $1 \pmod 4$. For a discriminant d, the Kronecker symbol $\left(\frac{d}{\cdot}\right)$ further extends the Jacobi symbol via

$$\left(\frac{d}{2}\right) = \begin{cases} 0, & \text{if } d \text{ is even;} \\ 1, & \text{if } d \equiv 1 (\bmod 8); \\ -1, & \text{if } d \equiv 5 (\bmod 8) \end{cases} \tag{2}$$

and by letting $\left(\frac{d}{-1}\right)$ be the sign of d. The value of $\left(\frac{d}{a}\right)$ is then defined for all integers a by multiplicativity, where we set $\left(\frac{d}{0}\right) = 0$ unless $d = 1$, in which case $\left(\frac{1}{0}\right) = 1$. By means of these extensions, the law of quadratic reciprocity (1) takes an elegant form for n positive and odd and any integer a:

$$\left(\frac{a}{n}\right) = \left(\frac{n^*}{a}\right), \tag{3}$$

where $n^* = (-1)^{\frac{n-1}{2}}\, n$. Note that n^* is a discriminant if n is odd.

3. The quadratic symbol for a finite group

Let G be a finite group of order n. An integer a that is prime to n acts as a permutation on the m conjugacy classes $C_1 = \{1\}, C_2, \ldots, C_m$

[1]We include the possibility that d is a square, which is usually disallowed.

of G by sending each element g to g^a. Define the quadratic symbol for G at any integer a by

$$\left(\frac{a}{G}\right) = \begin{cases} 0, & \text{if } (a,n) \neq 1; \\ 1, & \text{if this permutation is even;} \\ -1, & \text{if this permutation is odd.} \end{cases} \tag{4}$$

It is easy to see that $\left(\frac{\cdot}{G}\right)$ defines a real Dirichlet character $(\mathrm{mod}\, n)$.[2] Zolotarev's observation from the Introduction is that the quadratic symbol for $G = \mathbb{Z}/p\,\mathbb{Z}$ with an odd prime p is the Legendre symbol:

$$\left(\frac{a}{G}\right) = \left(\frac{a}{|G|}\right). \tag{5}$$

For any group G, a conjugacy class C is said to be real if $C^{-1} = C$ and complex otherwise. Here C^{-1} denotes the image of C under $g \mapsto g^{-1}$. Clearly the complex conjugacy classes occur in pairs $C \neq C^{-1}$ with $|C| = |C^{-1}|$. Let us order the conjugacy classes so that the first r_1 are real. Thus $m = r_1 + 2r_2$ where r_2 is half the number of complex conjugacy classes. Define

$$d = d(G) = (-1)^{r_2}|G|^{r_1}\prod_{j=1}^{r_1}|C_j|^{-1}. \tag{6}$$

This is a nonzero integer since for any conjugacy class C we have that $|G|/|C| = |C_G(g)|$, where $C_G(g)$ is the centralizer of any $g \in C$ [**2**, p.42]. It is clear that d is divisible by $n = |C_G(1)|$ and has the same prime divisors as n. We call d the discriminant of G, a name that is justified by the first statement of our main result.

THEOREM 1. *Let G be a finite group G with discriminant d as defined by (6). Then $d \equiv 0$ or $1 \pmod 4$, and for any integer a*

$$\left(\frac{a}{G}\right) = \left(\frac{d}{a}\right). \tag{7}$$

In particular, $\left(\frac{\cdot}{G}\right)$ is trivial if and only if d is a square.

In case G has odd order we have the following direct generalization of classical quadratic reciprocity (3):

COROLLARY 1. *If G has odd order n then $d = n^*$ and, for any integer a,*

$$\left(\frac{a}{G}\right) = \left(\frac{n^*}{a}\right). \tag{8}$$

Also, $\left(\frac{\cdot}{G}\right)$ is trivial if and only if n is a square.

[2]In fact, it is defined modulo the lcm of the orders of all elements of G.

It follows from (8) and (3) that Zolotarev's result (5) holds for any group G of odd order.

4. Proofs

The character table of G is the $m \times m$ matrix [**2**, p.59]:

$$M = \begin{pmatrix} \chi_1(C_1) & \dots & \chi_1(C_m) \\ \vdots & \ddots & \vdots \\ \chi_m(C_1) & \dots & \chi_m(C_m) \end{pmatrix}. \tag{9}$$

where $\chi_1 = 1, \chi_2 \dots, \chi_m$ are the irreducible (over $\mathbb{C}$) characters of G and we use the convention that $\chi(C) = \chi(g)$ for any $g \in C$. By the (second) orthogonality relations we have

$${}^t\bar{M}M = \begin{pmatrix} |G||C_1|^{-1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & |G||C_m|^{-1} \end{pmatrix}, \tag{10}$$

a diagonal matrix. Since $\chi(C^{-1}) = \bar{\chi}(C)$ for any character χ and any conjugacy class C, it is easy to see that

$$\det \bar{M} = (-1)^{r_2} \det M \tag{11}$$

and hence by (6) arrive at the identity

$$(\det M)^2 = \ell^2 d \tag{12}$$

for some $\ell \in \mathbb{Z}^+$.

Each entry $\chi_i(C_j)$ of M is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$. Now $\mathbb{Q}(\zeta_n)$ is a Galois extension of $\mathbb{Q}$ whose Galois group is isomorphic to $(\mathbb{Z}/n\,\mathbb{Z})^*$ by the map $\sigma_a \mapsto a$, with $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ acting on ζ_n by

$$\sigma_a(\zeta_n) = \zeta_n^a$$

[**6**, Theorem 1 p.92]. Using this, it is not difficult to check that

$$\sigma_a(\chi(g)) = \chi(g^a) \tag{13}$$

for any character χ and any $g \in G$.

To prove the first statement of Theorem 1, we apply an argument used by Schur [**8**] to prove Stickelberger's theorem about the discriminant of a number field. Observe that by the definition of the determinant

$$\det M = \sum \mathrm{sgn}(\rho)\chi_1(C_{\rho(1)})\chi_2(C_{\rho(2)}) \dots \chi_h(C_{\rho(n)}),$$

where the sum is over all permutations ρ of the integers $\{1, \dots, n\}$ and where $\mathrm{sgn}(\rho) = \pm 1$ according to whether ρ is even or odd. Write this as $A - B$, where A is the sum of the even permutations and B is the

sum of the odd permutations. By (13) both of the algebraic integers $A+B$ and AB are invariant under the Galois group and hence are ordinary integers. In particular, by (12)

$$\ell^2 d = (A-B)^2 = (A+B)^2 - 4AB \equiv (A+B)^2 \equiv 0, 1 \pmod 4,$$

proving the first statement.

It is apparent from (9) and (13) that

$$\sigma_a(\det M) = \left(\frac{a}{G}\right) \det M \tag{14}$$

and so by (12) we have

$$\sigma_a(\sqrt{d}) = \left(\frac{a}{G}\right) \sqrt{d}. \tag{15}$$

Since $\left(\frac{\cdot}{G}\right)$ is a character modulo n, to prove (7) it is enough to show it for $a = p$ with $p \nmid n$ and for $a = -1$. If $p \nmid n$ we use the Frobenius automorphism σ_p. It has the fundamental property that p splits completely in any subfield of $\mathbb{Q}(\zeta_n)$ if and only if σ_p fixes that subfield point-wise [**6**, p.91]. Thus p splits in $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ if and only if $\sigma_p(\sqrt{d}) = \sqrt{d}$.

We can always write the discriminant d as an integer square multiple of the discriminant $d_{\mathbb{K}}$ of $\mathbb{K}$, called a fundamental discriminant. Furthermore, p splits in $\mathbb{K}$ if and only if $\left(\frac{d_{\mathbb{K}}}{p}\right) = \left(\frac{d}{p}\right) = 1$ [**6**, p. 77]. Thus we have from (15) that

$$\left(\frac{p}{G}\right) = \left(\frac{d}{p}\right).$$

It is obvious from (11) and (6) that

$$\left(\frac{-1}{G}\right) = (-1)^{r_2} = \left(\frac{d}{-1}\right), \tag{16}$$

finishing the proof of (7). That $\left(\frac{\cdot}{G}\right)$ is nontrivial if d is not a square follows easily from Dirichlet's theorem on primes in progressions. Thus Theorem 1 is proven.

Suppose now that G has odd order n. Burnside [**1**, §222 p.294] observed that C_1 is the only real conjugacy class. To see this, suppose that g is in a real conjugacy class, so $h^{-1}gh = g^{-1}$ for some h. Then $h^{-2}gh^2 = g$ so $h^2 \in C_G(g)$. Since n is odd, the order of h is odd, say $2\ell+1$. It follows that $h = (h^2)^{\ell+1}$, so that $h \in C_G(g)$. Thus $g = g^{-1}$ so $g = 1$, since g has odd order.

Since $r_1 = 1$, it is clear from (6) that $d = (-1)^{\frac{m-1}{2}} n$. By the first statement of Theorem 1 we must have

$$d = (-1)^{\frac{n-1}{2}} n = n^*,$$

since n is odd.[3] The last statement of Corollary 1 follows from that of Theorem 1 since if n is odd then n^* is a square if and only n is a square.

5. Some examples

Let us compute the discriminants of some groups with even order. Suppose first that G is abelian and that the subgroup of G consisting of 1 and the elements of order 2 has order 2^t. Then $r_1 = 2^t$, so

$$d = (-1)^{\frac{n-2^t}{2}}\, n^{2^t}.$$

It follows that for G abelian of even order n, $\left(\frac{\cdot}{G}\right)$ is nontrivial if and only if $4 \,|\, n$ and $t = 1$, in which case for $(a, n) = 1$ we have

$$\left(\frac{a}{G}\right) = (-1)^{\frac{a-1}{2}}.$$

The condition $t = 1$ holds if G is cyclic, for instance.

In general, if G has only rational characters then it follows easily from (13) that $\left(\frac{\cdot}{G}\right)$ is the trivial character and hence that d is a square. This holds in particular for the symmetric group $G = S_k$, where one can also explicitly compute d.

On the other hand, it is not difficult to produce nonabelian groups with only real characters and with a nontrivial quadratic symbol. Consider, for example, the family of simple groups given by $G = \mathrm{SL}(2, \mathbb{F}_q)$ for $q = 2^r$ with $r > 1$. By [**7**, p.134 (= p.247)] we have that $n = q(q^2 - 1)$, that $m = r_1 = q + 1$ and that

$$d = q^2(q + 1)(q^2 - 1)^{q/2},$$

which is a square if and only if $r = 3$. If $r = 2$ we have that $G = A_5$ and $d_{\mathbb{K}} = 5$. For $r = 16$, $d_{\mathbb{K}} = 2^{16} + 1 = 65537$, a prime.

We would like to thank Jeffrey Stopple for his comments.

References

[1] W. Burnside, Theory of groups of finite order. 2d ed. Cambridge, 1911.
[2] C. W. Curtis, Pioneers of representation theory: Frobenius, Burnside, Schur and Brauer. AMS 1999
[3] F. G. Frobenius, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, Sber. Preuß. Akad. Berlin (1896) 689–703 (in Gesammelte Abhandlungen II, Springer-Verlag, Berlin 1968, 719–733)
[4] F. G. Frobenius, Über Gruppencharaktere, Sber. Preuß. Akad. Berlin (1896) 985–1021 (in Gesammelte Abhandlungen III, Springer-Verlag, Berlin 1968, 1–37)

[3] A stronger result discovered by Burnside [**1**, p.295] is that $n \equiv m \pmod{16}$.

[5] C. F. Gauss, Theorematis fundamentalis in doctrina de residuis quadraticus demonstrationes et ampliationes novæ, 1818 (in Werke II, 47-64.)
[6] P. Samuel, Algebraic theory of numbers. Translated from the French by Allan J. Silberger Houghton Mifflin Co., Boston, Mass. 1970
[7] I. Schur, Untersuchungen über die Darstellung der endliche Gruppen durch gebrochene lineare Substitutionen, J. für die reine und angew. Math. 132, 85–137 (1907) (#10 in Gesammelte Abhandlungen Band I , Springer-Verlag, New York 1973)
[8] I. Schur, Elementarer Beweis eines Satzes von L. Stickelberger, Math. Zeit. 29, 464–465 (1928) (#61 in Gesammelte Abhandlungen Band III , Springer-Verlag, New York 1973)
[9] G. Zolotarev, Nouvelle démonstration de la loi de réciprocité de Legendre, Nouvelles Ann. de Math. (2) 11 (1872), 354–362

William Duke
UCLA Mathematics Department
Box 951555
Los Angeles, CA 90095-1555
duke@math.ucla.edu

Kimberly Spears
UCSB Mathematics Department
Santa Barbara, CA 93106
kspears@umail.ucsb.edu